REPORT OF THE
MANHATTAN DISTRICT ATTORNEY'S
OFFICE ON

SMARTPHONE ENCRYPTION AND PUBLIC SAFETY

An update to the November 2017 Report

November 2018

Contents

Introduction

In September 2014, Apple Inc. ("Apple") announced that its latest operating system for smartphones and tablets would employ, by default, "full-disk encryption," which would render data on its devices completely inaccessible without a passcode, even to Apple, and even when sought via a court-ordered search warrant. Shortly, thereafter, Google followed suit.[1]

Since these announcements, this Office has written annual reports on the subject of smartphone encryption, to document the harmful impact these private business decisions have had on criminal investigations and criminal-justice outcomes, on the local, state, and national levels. In November 2015, we issued a white paper entitled *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*.[2] After summarizing the debate as it stood at the time, the 2015 Report explained the importance of evidence stored on smartphones; detailed how traditional investigatory methods cannot be used to unlock an encrypted device; and provided real-world examples of cases that were stymied and crimes that went unsolved as a result of these corporate decisions. It explained that, prior to Apple's 2014 announcement, there was no evidence that its devices were particularly susceptible to hacking, or that courts, when authorizing search warrants, were not properly protecting personal privacy interests as they have done for over two hundred years. Finally, our 2015 Report proposed a legislative solution that would provide a uniform national approach to balancing consumer privacy concerns and criminal justice needs, free from technology-company influence.[3]

Our 2016 Report further documented the unfolding impact of encryption on law enforcement and criminal justice, and the gathering debate (dominated largely by the technology companies themselves) about the supposed divide between criminal justice and privacy interests.[4] It also warned that continued legislative inaction would lead to an untenable "arms race" between tech companies and law enforcement, in which device manufacturers continually adopt technological "fixes" whenever law enforcement is able to access data through an ad-hoc "workaround."[5]

---

[1] Joe Miller, *Google and Apple to Introduce Default Encryption*, BBC, Sept. 19, 2014, *available at* https://www.bbc.com/news/technology-29276955

[2] *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*, Nov. 18, 2015, *available at* https://www.manhattanda.org/wp-content/themes/dany/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf

[3] *Id.* at 13.

[4] *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update to the November 2015 Report*, Nov. 17, 2016, *available at* https://www.manhattanda.org/wp-content/themes/dany/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf

[5] *Id.* at 7, 30.

Our 2017 Report examined this unfolding arms race, and explained that, despite law enforcement's ability to develop workarounds, such solutions are cost-prohibitive to most prosecutors and investigators, causing unequal access to justice for crime victims across the country.[6] The 2017 Report also provided examples of additional crimes—big and small—that went solved or unsolved depending on access to cellphone data, as well as cases where individuals were exonerated of serious crimes as a result of encrypted cellphone evidence.[7]

This is our Office's fourth annual Report. By way of overview, it begins with an update on the number and status of encrypted, inaccessible devices; recent examples of cases where cellphone evidence has been crucial; new developments in the U.S. courts; and legislative initiatives internationally. It goes on to examine the current state of the arms race between law enforcement and device makers, including a chronology of the continuing efforts by Apple to strengthen and enhance its encryption technology in the face of law-enforcement workarounds. The Report concludes with a discussion of the recent controversies that have plagued technology companies over their failures to protect consumer privacy, and why such developments only underscore the need for a legislative solution to the continuing encryption dispute.

I. The Continuing Encryption Problem: a 2018 Update

A. Cellphone Data Remains Critical to Solving Crimes and Exonerating the Innocent

It is beyond dispute that cellular telephones and other mobile devices contain essential evidence in a wide range of criminal cases, from identity theft to homicides, sexual offenses, and other violent crimes. For our Office and others, the number of inaccessible devices containing such evidence remains high. For example, in a recent four-month period, from May 2018 through August 2018, our Office's forensic lab, the High Technology Analysis Unit ("HTAU"), received 589 mobile devices in connection with live criminal investigations, 366 (or 62%) of which were passcode locked upon arrival at HTAU. As of this writing, of those 366 phones, nearly half (165) are still inaccessible.

---

[6] *Third Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*, Nov. 2017, *available at* https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption.pdf

[7] *Id.* at 3, 8-9.

The below charts provide more information on the crimes at issue and the devices received during this period.

Locked Phones and Tablets Received, by Crime Type

CRIME TYPE	MAY	JUNE	JULY	AUGUST	TOTAL
ASSAULT/ROBBERY/BURGLARY	12.7%	8.3%	14.9%	4.6%	10.0%
DRUG CHARGE	10.8%	13.9%	5.7%	18.3%	12.4%
HOMICIDE/ATTEMPTED MURDER	5.9%	9.7%	11.5%	13.8%	10.3%
LARCENY/FORGERY/FRAUD/CYBERCRIME ID THEFT	39.2%	34.7%	36.8%	32.1%	35.7%
OTHER	6.9%	2.8%	12.6%	2.8%	6.2%
SEX CRIME	16.7%	23.6%	17.2%	25.7%	20.8%
WEAPON CHARGE	7.8%	6.9%	1.1%	2.8%	4.6%

Phones and Tablets Received by HTAU

2017	2017 Total
LOCKED	48.9%
UNLOCKED	51.1%
2018	2018 Total
LOCKED	62.7%
UNLOCKED	37.3%

Regardless of the type of crime involved, these devices often contain evidence that is crucial to the prosecutors, officers, and agents trying to understand the facts of a given case. That evidence can, among other things, implicate a particular person in a crime, exonerate a person of criminal responsibility, or identify additional victims of a criminal scheme. As discussed in our 2017 Report, because gathering this data is essential to our mission, this Office has since 2014 been required, at great expense, to employ third-party companies that specialize in developing technological "workarounds" in an attempt to access encrypted devices that would otherwise be "warrant-proof." Below are just a few examples of cases handled by this Office over the past year in which smartphone evidence was particularly critical.

1. Cases Where Encrypted Data was Central to Proof of Guilt

- In one case, a defendant was identified as having shared child pornography online. Pursuant to a warrant, his encrypted mobile phone and other devices, including an encrypted external hard drive, were seized. Using a workaround, our Office was able to break into the phone and access its contents. A digital forensic technician then analyzed the phone's data, which contained password clues and use patterns. The technician was able to engineer the password for the hard drive using the phone data, and within the encrypted drive we discovered evidence that the defendant, a babysitter

who worked at a church, was not only sharing child pornography, but abusing children and recording the abuse as well. Based on the new evidence, our Office was able to charge the defendant with additional counts of Predatory Sexual Assault Against a Child and related charges. The defendant was convicted after trial, and sentenced to 100 years to life in prison.

- In another case, a defendant slashed a stranger in the face from behind and fled the scene of the crime. Video surveillance depicted an individual as he approached the victim, removed a razor blade from his mouth, slashed the victim on the face and fled. A suspect was arrested and his encrypted cellphone was obtained. Using a third-party workaround, we were able to access the phone, which revealed that, minutes after the slashing, the defendant sent an instant message which included an admission about cutting an individual as well as an image of a bloodied razor. The defendant subsequently plead guilty and was sentenced to twelve years in prison.

- In a similar incident, a defendant slashed a victim's face with a razor blade outside of a nightclub. After using a workaround to unlock the defendant's device, messages and videos on his phone established a motive for the crime. The device also contained threats by the defendant to act in the precise way that he did, as well as evidence that he had deliberately sought out the victim moments before the attack. The defendant subsequently plead guilty and was sentenced to eight years in prison.

The reality is, however, that workarounds do not always work. In other cases, we have been foreclosed from obtaining smartphone evidence because of the time it can take for software to unlock the device.

- In one such case, a defendant was convicted of having sexual intercourse with his biological daughter, a minor. A search warrant was obtained to search the defendant's phone, in the belief that it contained messages between the defendant and the victim that would establish a pattern of additional sexual assaults. The phone, however, was encrypted, and our Office, using a workaround, spent seven months attempting to unlock the device. Ultimately, these efforts proved unsuccessful, and additional crimes could not be charged.

- Earlier this year, a seven-month-old infant was found dead in the East River. The father of the child was found to have recently fled the country, and was subsequently apprehended abroad. A search warrant was obtained

authorizing a search of the defendant's devices, in the belief they would enable our Office to establish the time and manner of the infant's death. The devices, however, are encrypted, and, despite our best efforts, they remain inaccessible. As a result, the defendant has been charged with illegally disposing of the child's corpse, but the homicide itself remains unsolved.

- In a high-profile case, a defendant is charged with stalking and killing his ex-girlfriend. The police recovered his cellphone, which is believed to contain communications that could prove important at trial. The phone is encrypted, however, and—after six months of running an electronic workaround—the phone remains locked and no such evidence has been obtained.

2. Cases Where Encrypted Data Led to Exonerations

Of course, the value of smartphone evidence is not limited to proving a defendant's guilt. In some instances, evidence recovered from digital devices mitigates the culpability of an accused, or exonerates a defendant entirely. An internal survey of cases in our Office has identified seventeen cases in which we reduced or dismissed charges because of evidence we recovered from a smartphone.

- In one such case, two defendants were identified as part of a gang assault in which a large group of people attacked three men and two women. Two defendants who were present at the scene were identified as participants by an eyewitness. Based on evidence extracted from one of the defendant's phones, it was determined that the defendants were not present for the assault at all, and they were exonerated prior to trial.

- In a similar case, an individual was identified as being one of multiple participants in an attack, based on an independent eyewitness. The accused claimed to have been chatting with friends on a social media application from another friend's phone at the time. Based on data from the social media app, as well as cell site data for the phone, the defendant was shown to have been blocks away from the scene and not involved in the crime.

- In another case, a woman identified an individual as a person who had menaced her with a gun. The accused stated that he could not have committed the crime, because he had been in police custody at the time in connection with an unrelated matter. However, the accused could not corroborate his alibi. Through cell phone data and messages from the accused's social media

applications, investigators were able to locate the precinct where he had been detained, and the date and time of his detention, and were able to determine that he could not have committed the gun-related crime.

- In a firearms investigation, evidence recovered from a cellphone revealed that the phone's user was not, as originally believed, the person seen by police throwing a bag containing a loaded gun. The evidence recovered included: 1) photographs of the defendant from the date and time in question wearing a different outfit than the individual who was observed by the police, and 2) cell site data showing that the defendant was not in the area when the crime was committed.

Examples like these demonstrate that electronic evidence is critical to the truth-seeking mission of law enforcement, not only to prosecute the guilty, but also to exonerate the innocent. As users adopt smartphones for more and more of their communications needs, the importance of this evidence will continue to grow.

B. The Game of Cat and Mouse Continues

As described in our 2017 Report, Apple's and Google's encryption decisions have created a new market for private entities to develop and monetize encryption "workarounds."[8] Given the value of smartphone evidence across all types of criminal prosecutions, law enforcement agencies and federal and state prosecutors, including this Office, have availed themselves of these ad hoc third-party solutions, always with full notice to, and permission from, the judiciary. The associated costs to this and other law enforcement offices, which are ultimately passed on to taxpayers, is significant (for example, since 2015 this Office has paid third-party private vendors hundreds of thousands of dollars to attempt to unlock encrypted devices for use in criminal investigations). For those few offices with the resources to do so, the only option is to pay for such technology, given the value of the evidence on phones, even though, in many cases, the workarounds do not work at all. As we stated last year, the differences in law enforcement offices' ability to purchase such tools inevitably leads to an unequal system in which access to justice depends on the financial resources of a particular jurisdiction.

[8] A workaround "refers generally to any means by which law enforcement can access the plaintext (i.e. unencrypted) data on a device without assistance from the end user or the software manufacturer." *2017 Report* at 2; *see* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L.J. 989, 996-1011 (2018) (detailing six categories of encryption workarounds: "find the key, guess the key, compel the key, exploit a flaw in the encryption scheme, access plaintext when the device is in use, and locate a plaintext copy").

As predicted in our 2016 Report,[9] and as further discussed in our 2017 Report,[10] the advent of third-party workarounds has prompted device manufacturers to invent ever more complicated technologies to thwart the new means of access. The manufacturers' motivation in pursuing this "cat and mouse" approach is clear: as Apple recognized in its 2014 advertising, some percentage of iPhone purchasers will be attracted to a product that is impenetrable to law enforcement.[11] In short, the arms race has not only continued, it has intensified. Every time a workaround is developed, device manufacturers adjust their products accordingly.

A chronology of Apple's encryption decisions is as follows:

- In 2014, Apple announced that its new operating system, iOS 8, would employ "full disk encryption," meaning that Apple would not be able to access the contents of the devices it sold, even when served with a court order to do so.[12] As a result, for a phone that employed a four-digit passcode, it could take months for an office like ours, using third-party workarounds, to try to "crack" the code.

- Months later, when Apple announced iOS 9, it increased the default number of passcode digits to six, making it exponentially more difficult for law enforcement to determine the passcode (the potential combinations went from 10,000 to approximately one million,[13] and the time to possibly crack the code went from months to years).[14]

- Similarly, when Apple released iOS 11 in September 2017, it created even larger hurdles for law enforcement to search a locked phone: even when a device is unlocked using the user's fingerprint, it requires a passcode when an external device is connected. When the facial identification feature was added with the

---

[9] *2016 Report* at 30.
[10] *2017 Report* at 3.
[11] *See* Craig Timberg, *Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants*, Wash. Post, Sept. 18, 2014, *available at* https://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html?noredirect=on&utm_term=.cd10d57de4cd
[12] *Id.*; *see 2015 Report* at i and 1.
[13] Cyrus Farivar, *Apple to Require 6-Digit Passcode on Newer iPhones, iPads under iOS 9*, ARS Technica, June 8, 2015, *available at https://arstechnica.com/gadgets/2015/06/apple-to-require-6-digit-passcodes-on-newer-iphones-ipads-under-ios-9/* ("According to Apple (and math), this will vastly expand the effort required to crack a four-digit passcode. Instead of 10,000 possible combinations, newer iOS devices will soon have one million.").
[14] In one recent FBI investigation in Nebraska, an FBI agent obtained a search warrant for an Apple iPhone 6. However, the agent represented to the court that the FBI was unable to access the phone because the password decode "would take 28 years." Thomas Brewster, *Apple vs. GrayKey: Leaked Emails Expose the Fight for Your iPhone Privacy*, Forbes, July 26, 2018, *available at* https://www.forbes.com/sites/thomasbrewster/2018/07/26/apple-ios-security-boost-not-stopping-cops-hacking-iphones/#5c1949d27129

November 2017 release of iPhone X, it inherited this same security feature.[15] (This modification was announced after publicized reports that law enforcement had successfully obtained orders for users to provide their fingerprints.) This feature has substantially hindered law enforcement's ability to acquire data from a phone and create an image of the device, which is the best practice in cellphone forensic analysis.[16] Further, a "kill switch" was created by Apple to allow a user to temporarily disable Touch ID by pressing certain buttons on the phone, thus allowing a suspect approached by law enforcement to quickly disable the feature, making access for law enforcement even harder.[17]

- In July 2018, Apple released version iOS 11.4.1 of its operating system, which included a feature called USB Restricted Mode ("USB Mode").[18] Notably, this iOS version was released after the advent of new software that made workarounds significantly more accessible to law enforcement.[19] This feature,

---

[15] Jonny Evans, *iPhone X & Face ID: Everything You Need to Know*, Computerworld, Sept. 13, 2017, *available at* https://www.computerworld.com/article/3224569/apple-ios/iphone-x-and-face-id-everything-you-need-to-know.html; Chris Welch, *Apple Releases iOS 11.4.1 and Blocks Passcode Cracking Tools Used by Police*, The Verge, July 9, 2018, *available at* https://www.theverge.com/2018/7/9/17549538/apple-ios-11-4-1-blocks-police-passcode-cracking-tools

[16] *2017 Report* at 13 n. 44; Andy Greenberg, *Apple's IOS 11 Will Make it Even Harder for Cops to Extract Your Data*, Wired, Sept. 11, 2017, *available at* *https://www.wired.com/story/apples-ios-11-will-make-it-even-harder-for-cops-to-extract-your-data/* ("Since Apple locked down its iPhones three years ago with encryption that even the company itself can't break, it has been in a cold war with the cops—one that has occasionally turned hot. Exhibit A: its legal standoff with the FBI over the seized iPhone of San Bernardino killer Syed Rizwan Farook. Now, 18 months after that showdown, Apple is adding yet more features that are designed to guard your digital privacy from anyone who nabs your iPhone—whether it's a mugger on the street or the policeman who just threw you in jail.").

[17] Apple, *Use Emergency SOS on Your iPhone*, *available at* *https://support.apple.com/en-au/HT208076* ("If you use the Emergency SOS shortcut, you need to enter your passcode to re-enable Touch ID, even if you don't complete a call to emergency services.").

[18] Thomas Brewster, *Apple vs. GrayKey: Leaked Emails Expose the Fight for Your iPhone Privacy*, *supra* note 14.

[19] It was reported that GrayShift, a startup company cofounded by a former Apple engineer in 2016, has recently begun offering an iPhone unlock tool called GrayKey. *See* Thomas Brewster, *Mysterious $15,000 'GrayKey' Promises to Unlock iPhone X for the Feds*, Forbes, Mar. 5, 2018, *available at* https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack/#225681962950. The cost of using GrayKey is reportedly between $15,000 for an online version or $30,000 for an offline capability—amounts that have made the tool more affordable to law enforcement agencies. *Id.* Predictably, local, state and federal agencies have begun to purchase the GrayKey product. Joseph Cox, *Cops Around the Country Can Now Unlock iPhones, Records Show*, Vice Motherboard, Apr. 12, 2018, *available at* https://motherboard.vice.com/en_us/article/vbxxxd/unlock-iphone-ios11-graykey-grayshift-police. However, the cost of the unlock solution is only part of the expense associated with extracting data from a mobile device. Often, law enforcement requires experienced evidence technicians or forensic specialists to use forensic tools to extract data from the now-unlocked mobile device.

which is a default setting,[20] now specifies that "[i]f you don't first unlock your password-protected iOS device—or you haven't unlocked and connected it to a USB accessory within the past hour—your iOS device won't communicate with the accessory or computer . . . ."[21] Instead, a user is prompted to enter a passcode for the device to recognize and use the accessory to which it is connected.[22] What this means for law enforcement is that devices that connect through the USB port, as is required for most third-party workarounds, will now have to be connected within an hour of the phone being unlocked or the passcode will have to be entered.[23]

In contrast to Apple's advertising when it first announced its encryption policy in 2014 ("[u]nlike our competitors . . . it's not technically feasible for us to respond to governmental warrants . . ."),[24] Apple now claims that these subsequent encryption enhancements are not designed "to frustrate [law enforcement] efforts to do their jobs."[25] Whether or not this is true is beside the point. The fact is that device manufacturers have been steadfast in their defense of encryption technology year after year, whatever their economic motivation. As a result, the game of cat and mouse continues.[26]

C. An Update on Developments in the Courts

As discussed in our prior Reports, the question of whether and how law enforcement should be permitted to overcome encryption is not a question that realistically can be solved by our courts.[27] With regard to the compelled production of a user's passcode, the threshold question in litigation is whether such compelled production implicates a user's Fifth

---

[20] Chris Welch, *Apple Releases iOS 11.4.1 and Blocks Passcode Cracking Tools Used by Police*, *supra* note 15 ("If you go to Settings and check under Face ID (or Touch ID) & Passcode, you'll see a new toggle for USB Accessories. By default, the switch is off. This means that once your iPhone or iPad has been locked for over an hour straight, iOS will no longer allow USB accessories to connect to the device…").

[21] Apple, *Using USB Accessories with iOS 11.4.1 and Later*, *available at* https://support.apple.com/en-us/HT208857

[22] *Id.*

[23] Thomas Brewster, *Apple vs. GrayKey: Leaked Emails Expose the Fight for Your iPhone Privacy*, *supra* note 14.

[24] Craig Timberg, *Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants*, *supra* note 11.

[25] *See* Joseph Menn, *Apple to Undercut Popular Law-Enforcement Tool for Cracking iPhones*, Reuters, June 13, 2018, *available at* https://www.reuters.com/article/us-apple-iphone-cracking/apple-to-undercut-popular-law-enforcement-tool-for-cracking-iphones-idUSKBN1J92ZY

[26] *See* Jack Nicas, *Apple to Close iPhone Security Hole that Law Enforcement Uses to Crack Devices*, N.Y. Times, June 13, 2018, *available* at https://www.nytimes.com/2018/06/13/technology/apple-iphone-police.html ("Apple's latest move is part of a longer cat-and-mouse game between tech companies and law enforcement, said Michelle Richardson, an analyst at the Center for Democracy and Technology, which supports protections for online privacy. 'People always expected there would be this back-and-forth—that government would be able to hack into these devices, and then Apple would plug the hole and hackers would find another way in,' she said.").

[27] *See 2015 Report* at 5; *2016 Report* at 16-22; *2017 Report* at 10-14.

Amendment privilege against self-incrimination.[28] This issue has been addressed by a number of federal and state courts around the country, with no clear answer emerging.[29]

Even if a user properly invokes the Fifth Amendment, law enforcement may still be able to compel the user to decrypt a device by invoking the "foregone conclusion" doctrine.[30] If the government can demonstrate the "existence and location" of the privileged information, the Fifth Amendment does not apply, because it becomes an issue of "surrender," not "testimony."[31] However, as explained in both the 2016 and 2017 Reports, courts have typically applied two different approaches with regard to the "foregone conclusion" doctrine and decryption orders: 1) requiring the government to demonstrate that the contents of the device are known ahead of time;[32] or 2) demonstrating that the existence of the passcode, and the user's knowledge of it, are known facts.[33] A review of federal and state court decisions issued since the publication of our 2017 Report demonstrates that there has been no further indication of which line of reasoning will prevail,[34] with multiple courts requiring the more stringent first approach,[35] while others continue to apply the more permissive second approach.[36]

With respect to access using biometric data, starting with the iPhone X Apple has, at least temporarily, done away with Touch ID and now simply uses Face ID, which employs

---

[28] Additionally, as discussed in the 2017 Report, even where courts have compelled people to unlock devices, some individuals have opted to be held in contempt of court rather than complying with the orders, apparently believing that the punishment connected with the contents of the device may be worse than a contempt order. *See* Gloria Gomez, *Judge Jails Defendant for Failing to Unlock Phones*, Fox13, July 5, 2018, *available at* http://www.fox13news.com/news/local-news/judge-jails-man-for-failing-to-unlock-phones; Michael Todd, *Contempt and $22,000 Fine Ordered in Aptos Child Porn Case*, Santa Cruz Sentinel, Sept. 11, 2018, *available at* https://www.santacruzsentinel.com/2018/08/06/contempt-and-22000-fine-ordered-in-aptos-child-porn-case/.

[29] *See* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination (Sept. 12, 2018)*, Texas L. Rev., Forthcoming, USC Law Legal Studies Paper No. 18-15, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248286

[30] *See Fisher v. United States*, 425 U.S. 391, 411 (1976).

[31] *Id.* (citing *In re Harris*, 221 U.S. 274, 279 [1911] [internal quotations marks omitted]).

[32] *See In re Grand Jury Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1346-47 (11th Cir. 2012); *SEC v. Huang*, 2015 WL 5611644, at *2 (E.D. Pa. Sept. 23, 2015) (adopting the reasoning in *In re Grand Jury Duces Tecum Dated March 25, 2011).*

[33] *See State v. Stahl*, 206 So.3d 124, 135-37 (Fla. Dist. Ct. App. 2016); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 613-17 (Mass. 2014).

[34] Notably, the Supreme Court had an opportunity to weigh in on this issue. As discussed in the 2017 Report, the Third Circuit Court of Appeals affirmed a contempt order against a defendant who refused to comply with a court order to decrypt two hard drives. *See 2017 Report* at 11-12 (discussing *United States v. Apple Mac Pro Computer, et al.*, 851 F.3d 238 [3d Cir. 2017]). However, the Supreme Court denied petitioner's *writ of certiorari*. *Doe v. United States*, 138 S. Ct. 1988 (May 14, 2018).

[35] *See Seo v. Indiana*, __ N.E.3d__, 2018 WL 4040295 (Ind. Ct. App. 2018); *In re Matter of the Search of a Residence in Aptos, California 95003*, 2018 WL 1400401 (N.D. Cal. Mar. 20, 2018).

[36] *Commonwealth v. Davis*, 176 A.3d 869 (Pa. Super. Ct. 2017); *United States v. Spencer*, 2018 WL 1964588 (N.D. Cal. Apr. 26, 2018).

facial recognition to authenticate the user.[37] As described in our 2016 and 2017 reports,[38] biometric data such as fingerprints[39] or an individual's face is generally not considered to be protected by the Fifth Amendment. Since the 2017 Report, state and federal courts have continued to hold that law enforcement can order a user to unlock a device via a fingerprint sensor.[40]

Recently, it was reported that a duly authorized federal search warrant in Ohio was the "first known case in which law enforcement used Apple Face ID facial recognition technology to open a suspect's iPhone."[41] However, the affidavit filed in support of the warrant shows that Apple's recent updates still thwarted a complete forensic analysis of the phone even after it was unlocked using the suspect's face. That is because Apple now requires that the passcode be entered if the device has been locked for an hour or more and is subsequently connected to a computer.[42] As a result, the agent noted in his affidavit that, during his manual examination of the phone, he was unable to review all of the phone's information before it locked, and was unable to unlock it, since the passcode was unknown. Since he was able only to manually examine the phone, no deleted data was recovered.[43]

In short, recent cases continue to make clear that the encryption problem is not likely to be solved through litigation.

---

[37] Chaim Gartenberg, *Apple Reportedly Not Planning to Add In-Display Fingerprint Sensor on Upcoming iPhones*, The Verge, Sep. 4, 2018, *available at* https://www.theverge.com/circuitbreaker/2018/9/4/17819466/apple-fingerprint-sensor-iphone-face-id-rumor; Apple, *iPhone XS Face ID*, *available at* https://www.apple.com/iphone-xs/face-id/ ("Your face is your password").

[38] *2016 Report* at 18; *2017 Report* at 12-13

[39] *See* Thomas Brewster, *Yes, Cops Are Now Opening iPhones With Dead People's Fingerprints*, Forbes, Mar. 22, 2018, *available at* https://www.forbes.com/sites/thomasbrewster/2018/03/22/yes-cops-are-now-opening-iphones-with-dead-peoples-fingerprints/#763e6892393e

[40] *See State v. Diamond*, 905 N.W.2d 870 (Minn. 2018); *In re Matter of the Search of [Redacted] Washington, District of Columbia*, 317 F. Supp. 3d 523 (D.D.C. 2018).

[41] Thomas Brewster, *Feds Force Suspect to Unlock an Apple iPhone X with Their Face*, Forbes, Sept. 30, 2018, *available at* https://www.forbes.com/sites/thomasbrewster/2018/09/30/feds-force-suspect-to-unlock-apple-iphone-x-with-their-face/#b41288112597 (providing hyperlinks to the underlying affidavit in support of the search warrant and the warrant itself).

[42] *Id.* (Affidavit in Support at ¶ 49); Apple, *Using USB Accessories with iOS 11.4.1 and Later*, *supra* note 21.

[43] Thomas Brewster, *Feds Force Suspect to Unlock an Apple iPhone X with Their Face*, *supra* note 41 (Affidavit in Support at ¶ 50). Subsequent to Apple's introduction of USB Restricted Mode, it was reported that the United States Department of Justice is considering foregoing obtaining a warrant altogether and arguing that the one hour window imposed by Restricted Mode would allow the government to argue that "exigent circumstances" (i.e. the one hour window) permit a warrantless search of an unlocked phone. *See* Tim Starks, *Morning Cybersecurity: Defense Intelligence Agency Needs Focus on Cyber, House Panel Recommends*, Politico, June 14, 2018, *available at* https://www.politico.com/newsletters/morning-cybersecurity/2018/06/14/defense-intelligence-agency-needs-focus-on-cyber-house-panel-recommends-250920.

D. An Update on Developments Internationally

Consistent with discussions in our prior reports,[44] legislative and policy initiatives in other countries in the past year have continued to address, to varying degrees, potential solutions to the encryption debate. For example, the "Five Eyes" nations, consisting of the United States, the United Kingdom, Australia, New Zealand, and Canada, recently issued a joint statement calling on technology firms to provide lawful access to encrypted messages and communications.[45] The joint statement noted that, if impediments to access continue, "we may pursue technological, enforcement, legislative or other measures to achieve lawful access solutions."[46] As discussed below, some of these nations have already begun to take steps in this direction.

1. Australia

In September 2018, legislation was introduced in the Australian Parliament[47] that would require communications companies to provide assistance to law enforcement.[48] The Bill,[49] recognizing that the "increasing use of encryption has significantly degraded law enforcement and intelligence agencies' ability to access communications and collect intelligence, conduct investigations… and detect intrusions,"[50] requires communications providers in some instances to provide technical assistance to specific Australian law enforcement and intelligence agencies. The proposed legislation would impose fines of up to $10 million (Australian Dollars) on companies that fail to comply with technical assistance orders prescribed in the statute.[51] The proposed legislation received over fifteen thousand comments during the consultation period prior to its introduction in the legislature.[52] In

---

[44] *2015 Report* at 16-17; *2016 Report* at 27-28; *2017 Report* at 14-17.

[45] David E. Sanger & Sheera Frenkel, *'Five Eyes' Nations Quietly Demand Government Access to Encrypted Data*, N.Y. Times, Sept. 4, 2018, *available at* https://www.nytimes.com/2018/09/04/us/politics/government-access-encrypted-data.html

[46] *Id.*

[47] The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Parliament of Australia, *available at* https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195

[48] The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Australian Government, Department of Home Affairs, *available at* https://www.homeaffairs.gov.au/about/consultations/assistance-and-access-bill-2018

[49] http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6195_first-reps/toc_pdf/18204b01.pdf;fileType=application%2Fpdf. *See also* Erin Cooper, *Australia Plans Law for Tech Firms to Hand Over Encrypted Private Data*, Reuters, Aug. 14, 2018, *available at* https://www.reuters.com/article/us-australia-security-data/australia-plans-law-for-tech-firms-to-hand-over-encrypted-private-data-idUSKBN1KZ0W5

[50] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 Explanatory Memorandum, House of Representatives of the Commonwealth of Australia, *available at* http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6195_ems_1139bfde-17f3-4538-b2b2-5875f5881239/upload_pdf/685255.pdf;fileType=application%2Fpdf

[51] *Id.* at § 317ZB(2).

[52] Australian Government, Department of Home Affairs, *Parliamentary Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (2018), at 41. A committee hearing on the bill has

October 2018, the Alliance for a Safe and Secure Internet, an industry organization representing Apple, Facebook, Google, and Amazon, announced their opposition to the Australia legislation.[53]

2. France

The French Supreme Court recently heard, and rejected, a challenge to 2016 legislation that created an offense for refusal to provide a decryption key for a device that law enforcement knows exists and suspects was used in the commission of crime.[54] Article 434-15-2 of the French Penal Code makes such refusal to punishable by three years imprisonment and a fine of 270,000€, as well as an increase to five years and 450,000€ if decryption would have prevented a crime.[55] The court found this Article to be constitutional, following the rationale that the act of providing a decryption key does not presume a defendant's guilt, nor does it violate the right against self-incrimination because the data already exists on the device.[56]

3. United Kingdom

The Investigatory Powers Bill, discussed in our two previous reports, was passed into law[57] but remains subject to a legal challenge that it is incompatible with European privacy law.[58] In light of conflicts with new laws regarding access to retained data and judicial review of data requests, the judges hearing the case have given authorities six months to provide a new draft that conforms with those principles.[59]

---

been scheduled for October 19, 2018, and has received over sixty comment submissions from individuals, government groups, and other organizations.

[53] Colin Packham, *Tech Giants Allied Against Proposed Australia Law Seeking Encrypted Data*, Reuters, Oct. 3, 2018, *available at* https://www.reuters.com/article/us-australia-security-data/tech-giants-allied-against-proposed-australia-law-seeking-encrypted-data-idUSKCN1MD0CI

[54] Conseil Constitutionnel, Décision n° 2018-696 QPC du 30 mars 2018, *available at* https://www.conseil-constitutionnel.fr/decision/2018/2018696QPC.htm

[55] Art. 434-15-2 C. pén.

[56] Conseil Constitutionnel, Décision n° 2018-696 QPC du 30 mars 2018, *available at* https://www.conseil-constitutionnel.fr/decision/2018/2018696QPC.htm

[56] *Id.*

[57] *Investigatory Powers Act 2016*, U.K. Parliament, *available at* https://services.parliament.uk/bills/2015-16/investigatorypowers.html

[58] Ian Cobain, *UK Has Six Months to Rewrite Snooper's Charter, High Court Rules*, Guardian, Apr. 27, 2018, *available at* https://www.theguardian.com/technology/2018/apr/27/snoopers-charter-investigatory-powers-act-rewrite-high-court-rules

[59] *Id.*

II. The Evolving Privacy Debate: Technology Companies Have Been Increasingly Criticized for Putting Profits Ahead of Security

In the absence of Congressional oversight, technology companies like Apple, Google and others have effectively established themselves as the arbiters of what data they can and should collect, and how they should or should not make that data available pursuant to legal process. As noted above, upon the advent of full-disk encryption in 2014, Apple advertised to potential buyers of iPhones that its new operating system would be impenetrable, even to law enforcement, even with a judicially issued warrant.[60] Since then, encryption efforts by device makers have intensified year after year, and many consumers and commentators have responded with enthusiasm to the claim that tech companies are an important bulwark in the protection of consumer privacy interests.

In the past year, however, a number of high-profile controversies have called public attention to the fact that certain technology companies have made their decisions, not based on what might be prudent public policy, but—understandably—based on what is in their shareholders' economic interest.[61] In response, Bill Gates, the founder of Microsoft, has publicly warned other tech companies to "be careful that they're not . . . advocating things that would prevent government from being able to, under appropriate review, perform the type of functions that we've come to count on," such as advocating "that even a clear mass-murdering criminal's communication should never be available to the government."[62]

One of the most widely-covered of these controversies involved Cambridge Analytica, a British political consulting firm, and Facebook.[63] In March 2018, it was reported that

---

[60] *See 2015 Report* at 1; *see* Craig Timberg, *Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants*, *supra* note 11 ("Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data," Apple said on its Web site. "So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8.").

[61] *See* Kalev Leetaru, *Profit Versus Privacy: Facebook's Stock Collapse and It's Empty 'Privacy First' Promise*, Forbes, July 29, 2018, *available at* https://www.forbes.com/sites/kalevleetaru/2018/07/29/profit-versus-privacy-facebooks-stock-collapse-and-its-empty-privacy-first-promise/#509456457879; Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not*, Associated Press, Aug. 13, 2018, *available at* *https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not*

[62] Mike Allen, *Bill Gates: Tech Companies Inviting Government Intervention*, Axios, Feb. 13, 2018, *available at* https://www.axios.com/bill-gates-warns-big-tech-1518515340-fa3aa353-6078-405b-b3aa-8252bd06c1fc.html. Notably, Tim Cook, Apple's Chief Executive Officer, recently "lashed into Silicon Valley competitors that collect user data, equating their services to 'surveillance[,]'" arguing that "these stockpiles of data serve only to make rich the companies that collect them." Natalia Drozdiak & Stephanie Bodoni, *Tim Cook Takes Aim at Companies That Stockpile Private Data*, Bloomberg, Oct. 24, 2018, *available at* https://www.bloomberg.com/news/articles/2018-10-24/apple-ceo-preaches-importance-of-privacy-at-eu-conference

[63] Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. Times, Mar. 17, 2018, *available at* https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html; Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. Times, Mar. 19,

Cambridge Analytica had improperly gained access to the private information of more than 50 million Facebook users.[64] The information included Facebook users' friend networks, "likes," details on the users' identity and location.[65] Cambridge Analytica harvested this data with analytical tools that could identify the personalities of American voters and used it for political purposes. The company sold its analysis to political campaigns, including President Trump's 2016 campaign, and provided data to foreign and domestic politicians, including those involved in "Brexit"—Britain's referendum to leave the European Union–for use in their efforts to influence public opinion.[66] These reports, which called into question how Facebook collects and handles the private information of its users, led to congressional hearings and calls for increased oversight of social media companies.

After the Cambridge Analytica story broke, Facebook also disclosed that an attack on its computers had exposed the private data of nearly 30 million of its users.[67] The hackers attempted to retrieve users' private data, including name, sex and hometown. This latest breach again brought calls to Congress and the Federal Trade Commission to take action that would protect the privacy and security of social media users.[68]

But Facebook is not the only technology company to have its handling of users' data called into question. Recently, as alleged in a complaint filed by the New Mexico Attorney General, children using various children's apps had their user data, including the location of their devices, collected without their knowledge by the makers of the apps.[69] The lawsuit accuses an app maker, along with online ad businesses run by Google and Twitter, of violating the federal Children's Online Privacy Protection Act.

In the summer of 2018, it was reported that Google was planning on launching a censored version of its search engine in China.[70] The project, code-named Dragonfly, would

---

2018, *available at* https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

[64] Shortly thereafter, Facebook announced that it was actually 87 million Facebook users, including 70 million in the United States. *See* Nadeem Badshah, *Facebook to Contact 87 Million Users Affected by Data Breach*, The Guardian, Apr. 8, 2018, *available at* https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach

[65] Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, *supra* note 63.

[66] *Id.*

[67] *See* Guy Rosen, *An Update on the Security Issue*, Facebook Newsroom, Oct. 12, 2018, *available at* https://newsroom.fb.com/news/2018/10/update-on-security-issue/ (noting that although Facebook initially believed that 50 million people were affected, the number was closer to 30 million).

[68] Mike Issac & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. Times, Sept. 28, 2018, *available at* https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html?login=email&auth=login-email

[69] Jennifer Valentino-DeVries, Natasha Singer, Aaron Krolik & Michael H. Keller, *How Game Apps That Captivate Kids Have Been Collecting Their Data*, N.Y. Times, Sept. 12, 2018, *available at* https://www.nytimes.com/interactive/2018/09/12/technology/kids-apps-data-privacy-google-twitter.html

[70] Ryan Gallagher, *Google Plans to Launch Censored Search Engine in China, Leaked Documents Reveal*, The Intercept, Aug. 1, 2018, *available at* https://theintercept.com/2018/08/01/google-china-search-engine-censorship/. As

restrict website and search terms dealing with democracy, human rights, peaceful protest, and religion.[71] Google previously had maintained a censored version of its search engine in China, but in 2010 the company pulled out, citing cyber-attacks originating from China that apparently succeeded in accessing the Gmail accounts of Chinese human rights activists, along with China's blocking of websites such as Facebook, Twitter, and YouTube.[72] Nonetheless, Dragonfly would apparently create a new custom Android app that would comply with China's strict censorship laws.[73] This proposed decision has been met with great resistance, both inside[74] and outside Google.[75]

On August 3, 2018, in response to various news reports about Google's plan to launch Dragonfly in China, a bipartisan group of United States Senators wrote Google to voice their concern, stating that the "reported plan is deeply troubling and risks making Google complicit in human rights abuses related to China's rigorous censorship regime."[76] Google responded later that month, stating that the issue of whether it could or would release a search engine in China remains unclear, and that they were "not in a position to be able to answer detailed questions."[77] One Senator stated he was "truly disappointed" by Google's response.[78] Others called upon Google to cease its development of Dragonfly, arguing that the app "will

---

noted in our 2017 Report, notwithstanding privacy concerns, Apple complied with the Chinese government's directives that businesses locate their servers within mainland China. *2017 Report* at 6–7; *see* Cory Bennett & Katie Bo Williams, *Apple Defends China Moves Amid FBI Spat*, The Hill, Mar. 20, 2016, *available at* https://thehill.com/policy/cybersecurity/273629-apple-defends-china-moves-amid-fbi-spat

[71] Ryan Gallagher, *Google Plans on Launch Censored Search Engine in China, Leaked Documents Reveal*, *supra* note 70.

[72] *A New Approach to China: an update*, Google Official Blog, Mar. 22, 2010, *available at* https://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html

[73] Ryan Gallagher, *Google Plans to Launch Censored Search Engine in China, Leaked Documents Reveal*, *supra* note 70.

[74] *Id.*; Kate Conger & Daisuke Wakabayashi, *Google Employees Protest Secret Work on Censored Search Engine for China*, N.Y. Times, Aug. 16, 2018, *available at* https://www.nytimes.com/2018/08/16/technology/google-employees-protest-search-censored-china.html.

[75] Kara Swisher, *The Real Google Censorship Scandal*, N.Y. Times Opinion, Sept. 13, 2018, *available at* https://www.nytimes.com/2018/09/13/opinion/google-censorship-trump-china.html?action=click&module=Opinion&pgtype=Homepage&login=email&auth=login-email

[76] Letter from Marco Rubio, Tom Cotton, Mark R. Warner, Ron Wyden, Cory Gardner & Robert Menendez, United States Senators, to Mr. Sundar Pichai, Chief Executive Officer, Google, LLC, Aug. 3, 2018, *available at* https://www.rubio.senate.gov/public/_cache/files/9b139bf6-d0c1-4969-aaf2-4a4aede8ed35/397FE4632728A13B6EEABDB5956550AC.8-3-18-letter-to-mr.-pichai-re-censorship-in-china.pdf; *see* Erik Wasson, *Google Slammed by Senators Over Censored China Search Engine*, Bloomberg, Aug. 3, 2018, *available at* https://www.bloomberg.com/news/articles/2018-08-03/google-slammed-by-senators-over-censored-search-engine-for-china

[77] Letter from Sundar Pichai, Chief Executive Officer, Google, LLC, to Marco Rubio, Tom Cotton, Mark R. Warner, Ron Wyden, Cory Gardner & Robert Menendez, United States Senators, Aug. 31, 2018, *available at* https://freebeacon.com/wp-content/uploads/2018/09/Pichai-Response-to-Senators-Regarding-China.pdf

[78] *The Latest: Senator Blasts Google for Reply on China Search*, Associated Press, Sept. 4, 2018, *available at* https://www.apnews.com/a51af23a42fb46059a1dfe5c48e7e50a/The-Latest:-Senator-blasts-Google-for-reply-on-China-search

strengthen Communist Party censorship and compromise the privacy of Chinese customers."[79]

Even more recently, it was reported that a number of Google services on iPhones and Android devices have been storing user location data, even if the user selected a privacy setting that purportedly prevented Google from doing so.[80] Critics argued that this tracking of location information was driven by Google's attempt to boost advertising revenue.[81] In October 2018, it was further disclosed that the private data of hundreds of thousands of Google+ users was exposed to outside developers.[82] Upon learning this, Google decided against disclosing the privacy breach, fearing that the incident "would likely trigger 'immediate regulatory interest' and invite comparisons to Facebook's leak of user information to data firm Cambridge Analytica."[83]

In response to calls for greater regulation of technology companies' handling of consumer data, the European Union this year instituted the General Data Protection Regulation (GDPR),[84] which imposes stringent privacy regulations on the collection, maintenance, and use of internet users' personal information.[85] The regulation requires businesses and online platforms to provide clear and simplified terms and conditions for websites, obtain consent from users in order to process their personal information, and limit the retention of personal data.[86] The GDPR also provides strict requirements for the transfer of personal information to third parties, especially those in countries outside of the European Union.[87]

---

[79] Michael C. Bender & Dustin Volz, *Pence Calls on Google to Drop Mobile Search Project in China*, Wall St. J., Oct. 4, 2018, *available at* https://www.wsj.com/articles/pence-calls-on-google-to-drop-mobile-search-project-in-china-1538680844

[80] Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not*, *supra* note 61.

[81] *Id.*

[82] Douglas MacMillan & Robert McMillan, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, Wall St. J., Oct. 8, 2018, *available at* https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194?mod=hp_lead_pos1.

[83] *Id.*

[84] Regulation (EU) 2016/679; *Data Protection in the EU*, European Comm'n, *available at* https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en; *see generally* Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. Times, May 24, 2018, *available at* https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html

[85] *See* Adam Satariano, *What the G.D.P.R., Europe's Tough New Data Law, Means for You*, N.Y. Times, May 6, 2018, *available at* https://www.nytimes.com/2018/05/06/technology/gdpr-european-privacy-law.html

[86] Regulation (EU) 2016/679.

[87] *Id.* The GDPR does not address the ability of governments or law enforcement to access data stored by technology companies. Scholars have raised the potential conflict between the GDPR and U.S. statutes governing requests for digital information (*see* Brief of EU Data Protection and Privacy Scholars as amici curiae in support of respondent, *United States v. Microsoft*, No. 17-2, at 2) and British investigatory laws have already conflicted with European data privacy policies and are currently subject to ongoing challenge. Thus, while this legislation marks a step towards the protection of citizens' digital data, legislative action remains necessary to clarify when and how technology companies must comply with lawful government orders.

The GDPR had an immediate impact on businesses and platforms with an online presence in European Union member countries, as companies who do not comply may face significant fines, which may reach as high as 20 million Euros, or four percent of the company's "worldwide annual turnover" for the preceding year.[88] Although much of the practical enforcement of GDPR provisions is yet to be seen (it has been in effect less than six months at the time of publication), the new law has already had a substantial impact on businesses that have updated terms of use and privacy policies and implemented mechanisms to obtain user consent to comply.[89]

* * *

In short, notwithstanding their public pronouncements about their role in protecting the privacy of customers, it is important to understand that technology companies are obliged to act in the economic interests of their shareholders, and that they are, in many important ways, unregulated when it comes to their handling of customer data. It follows that such companies should not be relied upon to act as the principal gatekeepers and decision-makers on significant public policy questions of how and when customer data should be made available for criminal justice or public safety purposes.

III. Federal Legislation Remains the Only Answer

Recognizing that a solution to the encryption problem is not going to come from private industry or the courts, our initial Report in 2015 recommended an across-the-board legislative solution (including draft statutory language) that would reconcile privacy interests with the need for judicially-sanctioned access in appropriate cases:

> "Congress should enact a statute that requires any designer of an operating system for a smartphone or tablet manufactured, leased or sold in the U.S. to ensure that data on its devices is accessible pursuant to a search warrant. Such a law would be well within Congress's Commerce Clause powers, and does not require costly or difficult technological innovations."[90]

For the reasons advanced in each of our prior Reports, national legislation of the sort we have proposed remains the most rational and least intrusive means to require device manufacturers to comply with lawful court orders in serious criminal cases upon a finding of probable cause.

Importantly, this would not be the first time Congress enacted a law that addressed an entire sector as a means ensure the ability to investigate and prosecute crimes. In 1970, in response to large amounts of cash coming into the country's financial institutions, Congress

---

[88] *See* Adam Satariano, *What the G.D.P.R., Europe's Tough New Data Law, Means for You*, *supra* note 85.

[89] *See, e.g.*, Brian X. Chen, *Getting a Flood of G.D.P.R.-Related Privacy Policy Updates? Read Them*, N.Y. Times, May 23, 2018, *available at* https://www.nytimes.com/2018/05/23/technology/personaltech/what-you-should-look-for-europe-data-law.html

[90] *2015 Report* at ii; *id.* at Appendix 1 (draft statutory language); *see 2016 Report* at 29-32; *2017 Report* at 17-18.

passed the Bank Secrecy Act ("BSA"), otherwise known as the Currency and Foreign Transaction Reporting Act.[91] The BSA required financial institutions to adopt anti-money laundering programs to help identify the source, volume, and movement of currency through the United States financial system. To ensure the law's objectives, the BSA mandated that financial institutions keep certain standard records and report suspicious financial activity identified by compliance professionals to law enforcement.[92]

Similarly, in 1994, recognizing a law enforcement need for uniform data and a means to intercept communications over digital telephone networks, Congress passed the Communications Assistance for Law Enforcement Act ("CALEA").[93] In particular, CALEA standardized the data that equipment manufacturers and telecommunications providers were required to keep, established a data retention period, and required telecommunications manufacturers and carriers "to ensure that they have the necessary surveillance capabilities to comply with legal requests for information."[94] At the time of its enactment, CALEA applied to landline and cellular telecommunications carriers, and it was amended in 2006 to include Voice over Internet Protocol ("VoIP") and broadband internet providers. Today, however, CALEA has not kept pace with technological innovation and does not apply to device manufacturers, which now perform the same or similar functions as telecommunications carriers.

Whether achieved as an amendment to CALEA, or in the form of the proposed Compliance with Court Orders Act of 2016,[95] or via the simple statutory language our Office has previously proposed,[96] legislation of this sort would be well within Congress' authority to implement. The companies that manufacture our cellphones and related devices control access to information that is vital to the lives of millions of Americans, and they do so without the regulation and oversight that is common across other industries where there is a need to protect public safety and guard against abuse. Such oversight remains sorely needed, and our Office stands willing to assist Congress and all relevant stakeholders in the effort to find a more rational balance among the interests of device makers, consumers and law enforcement in the regulation of smartphone encryption.

---

[91] *See* United States Treasury, Financial Crimes Enforcement Network, *History of Anti-Money Laundering Laws*, *available at* https://www.fincen.gov/history-anti-money-laundering-laws

[92] *Id.*

[93] 47 U.S.C. § 1001 et seq.

[94] Federal Communications Commission, *Communications Assistance for Law Enforcement Act*, *available at* https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance

[95] *2016 Report* at 23, 32. A discussion draft of the bill was made available to the public in a press release issued by Senator Dianne Feinstein on April 13, 2016, *available at* https://www.feinstein.senate.gov/public/_cache/files/5/b/5b990532-cc7f-427f-9942-559e73eb8bfb/6701CF2828167CB85F51D12F7CB69D74.bag16460.pdf; *2016 Report* at 23, 31.

[96] *See 2015 Report* at 13, n. 31; *2016 Report* at 32.